THE MORDELL-LANG THEOREM FOR FINITELY GENERATED SUBGROUPS OF A SEMIABELIAN VARIETY DEFINED OVER A FINITE FIELD

DRAGOS GHIOCA

Abstract. We determine the structure of the intersection of a finitely generated subgroup of a semiabelian variety G defined over a finite field with a closed subvariety $X \subset G$.

1. Introduction

Let G be a semiabelian variety defined over a finite field $\mathbb{F}_q$. Let K be a regular field extension of $\mathbb{F}_q$. Let F be the corresponding Frobenius for $\mathbb{F}_q$. Then $F \in \mathrm{End}(G)$.

Let X be a subvariety of G defined over K (in this paper, all subvarieties will be closed). In [3] and [4], Moosa and Scanlon discussed the intersection of the K-points of X with a finitely generated $\mathbb{Z}[F]$-submodule Γ of $G(K)$. They proved that the intersection is a finite union of *F-sets* in Γ (see Definition 2.4). Our goal is to extend their result to the case when Γ is a finitely generated subgroup of $G(K)$ (not necessarily invariant under F).

In Section 2 we will state our main results, which include, besides the Mordell-Lang statement for subgroups of semiabelian varieties defined over finite fields, also a similar Mordell-Lang statement for Drinfeld modules defined over finite fields. The Mordell-Lang Theorem for Drinfeld modules was also studied by the author in [1]. In Section 3 we will prove our main theorem for semiabelian varieties, while in Section 4 we will show how the Mordell-Lang statement for Drinfeld modules defined over finite fields can be deduced from the results in [3]. We will conclude Section 4 with two counterexamples for two possible extensions of our statement for Drinfeld modules towards results similar with the ones true for semiabelian varieties.

2. Statement of our main results

Everywhere in this paper, $\overline{Y}$ represents the Zariski closure of the set Y.

A central notion for the present paper is the notion of a *Frobenius ring*. This notion was first introduced by Moosa and Scanlon (see Definition 2.1 in [4]). We extend their definition to include also rings of finite characteristic.

Definition 2.1. Let R be a Dedekind domain with the property that for every nonzero prime ideal $\mathfrak{p} \subset R$, $R/\mathfrak{p}$ is a finite field. We call $R[F]$ a Frobenius ring if the following properties are satisfied:

(i) $R[F]$ is a simple extension of R generated by a distinguished element F.

(ii) $R[F]$ is a finite integral extension of R.

(iii) F is not a zero divisor in $R[F]$.

(iv) The ideal $F^{\infty}R[F] := \bigcap_{n\geq 0} F^n R[F]$ is trivial.

[1]2000 AMS Subject Classification: Primary 11G10; Secondary 11G09, 11G25

The classical example of a Frobenius ring associated to a semiabelian variety G defined over the finite field $\mathbb{F}_q$ is $\mathbb{Z}[F]$, where F is the corresponding Frobenius for $\mathbb{F}_q$. This Frobenius ring is discussed in [3] and [4]. We will show later in this section that $A[F]$ is also a Frobenius ring when F is the Frobenius on $\mathbb{F}_q$ and $\phi : A \to \mathbb{F}_q[F]$ is a Drinfeld module (in this case, A is a Dedekind domain of finite characteristic).

We define the notion of *groupless F-sets* contained in a module over a Frobenius ring.

Definition 2.2. Let $R[F]$ be a Frobenius ring and let M be an $R[F]$-module. For $a \in M$ and $\delta \in \mathbb{N}^*$, we denote the F^δ-orbit of a by $S(a;\delta) := \{F^{\delta n}a \mid n \in \mathbb{N}\}$. If $a_1, \ldots, a_k \in M$ and $\delta_1, \ldots, \delta_k \in \mathbb{N}^*$, then we denote the sum of the F^{δ_i}-orbits of a_i by

$$S(a_1, \ldots, a_k; \delta_1, \ldots, \delta_k) = \{\sum_{i=1}^{k} F^{\delta_i n_i} a_i \mid (n_1, \ldots, n_k) \in \mathbb{N}^k\}.$$

A set of the form $b + S(a_1, \ldots, a_k; \delta_1, \ldots, \delta_k)$ with $b, a_1, \ldots, a_k \in M$ is called a groupless F-set based in M. We do allow in our definition of groupless F-sets $k = 0$, in which case, the groupless F-set consists of the single point b. We denote by GF_M the set of all groupless F-sets based in M. For every subgroup $\Gamma \subset M$, we denote by $\mathsf{GF}_M(\Gamma)$ the collection of groupless F-sets contained in Γ and based in M. When M is clear from the context, we will drop the index M from our notation.

Remark 2.3. Each groupless F-set O is based in a finitely generated $\mathbb{Z}[F]$-module.

Definition 2.4. Let M be a module over a Frobenius ring $R[F]$. Let $\Gamma \subset M$ be a subgroup. A set of the form $(C + H)$, where $C \in \mathsf{GF}_M(\Gamma)$ and H is a subgroup of Γ invariant under F is called an F-set in Γ based in M. The collection of all such F-sets in Γ is denoted by $\mathsf{F}_M(\Gamma)$. When M is clear from the context, we will drop the index M from our notation.

Let G be a semiabelian variety defined over $\mathbb{F}_q$. Let F be the corresponding Frobenius for $\mathbb{F}_q$. Let K be a finitely generated regular extension of $\mathbb{F}_q$. We fix an algebraic closure K^{alg} of K. Let Γ be a finitely generated subgroup of $G(K)$. We denote by $\mathsf{F}(\Gamma)$ and $\mathsf{GF}(\Gamma)$ the collection of F-sets and respectively, the collection of groupless F-sets in Γ based in $G(K^{\mathrm{alg}})$ (which is obviously a $\mathbb{Z}[F]$-module). When we do not mention the $\mathbb{Z}[F]$-submodule containing the base points for the F-sets contained in Γ, then we will always understand that the corresponding submodule is $G(K^{\mathrm{alg}})$. The following theorem is our main result for semiabelian varieties.

Theorem 2.5. *Let G, K and Γ be as in the above paragraph. Let X be a K-subvariety of G. Then $X(K) \cap \Gamma = \bigcup_{i=1}^{r}(C_i + H_i)$, where $(C_i + \Delta_i) \in \mathsf{F}(\Gamma)$. Moreover, the subgroups Δ_i from $X(K) \cap \Gamma$ are of the form $G_i(K) \cap \Gamma$, where G_i is an algebraic subgroup of G defined over $\mathbb{F}_q$.*

As mentioned in Section 1, the result of our Theorem 2.5 was establised in [3] (see Theorem 7.8) and in [4] (see Theorem 2.1) for finitely generated $\mathbb{Z}[F]$-modules $\Gamma \subset G(K)$. Because $\mathbb{Z}[F]$ is a finite extension of $\mathbb{Z}$, each finitely generated $\mathbb{Z}[F]$-module is also a finitely generated group (but *not* every finitely generated group is invariant under F).

We describe now the setting for our Drinfeld modules statements. We start by defining Drinfeld modules over finite fields.

Let p be a prime number and let q be a power of p. Let C be a projective nonsingular curve defined over $\mathbb{F}_q$. We fix a closed point ∞ on C. Let A be the ring of $\mathbb{F}_q$-valued functions on

C, regular away from ∞. Then A is a Dedekind domain. Moreover, A is a finite extension of $\mathbb{F}_q[t]$. Hence, for every nonzero prime ideal $\mathfrak{p} \subset A$, $A/\mathfrak{p}$ is a finite field.

Let F be the corresponding Frobenius on $\mathbb{F}_q$. We call a Drinfeld module defined over $\mathbb{F}_q$ a ring homomorphism $\phi : A \to \mathbb{F}_q[F]$ such that there exists $a \in A$ for which $\phi_a := \phi(a) \notin \mathbb{F}_q \cdot F^0$ (i.e. the degree of ϕ_a as a polynomial in F is positive). In general, for every $a \in A$, we write ϕ_a to denote $\phi(a) \in \mathbb{F}_q[F]$. We note that this is not the most general definition for Drinfeld modules defined over finite fields (see Example 4.8).

For each field extension L of $\mathbb{F}_q$, ϕ induces an action on $\mathbb{G}_a(L)$ by $a * x := \phi_a(x)$ for every $x \in L$ and for every $a \in A$. For each $g \geq 1$, we extend the action of A diagonally on $\mathbb{G}_a^g$.

Clearly, for every $a \in A$, $F\phi_a = \phi_a F$. This means F is an *endomorphism* of ϕ (see Section 4 of Chapter 2 in [2]). We let $A[F] \in \mathrm{End}(\phi)$ be the finite extension of A generated by F, where we identified A with its image in $\mathbb{F}_q[F]$ through ϕ. Actually, $A[F]$ is isomorphic to $\mathbb{F}_q[F]$. However, we keep the notation $A[F]$ instead of $\mathbb{F}_q[F]$, when we talk about modules over this ring only to emphasize the Drinfeld module action given by A.

Lemma 2.6. *The ring $A[F]$ defined in the above paragraph is a Frobenius ring.*

Proof. Because for some $a \in A$, ϕ_a is a polynomial in F of positive degree, we conclude F is integral over A. Because $\mathbb{F}_q[F]$ is a domain, we conclude F is not a zero divisor. Also, no nonzero element of $A[F]$ is infinitely divisible by F because all elements of $A[F]$ are polynomials in F and so, no nonzero polynomial can be infinitely divisible by some polynomial of positive degree. Therefore $A[F]$ is a Frobenius ring. □

Let K be a regular field extension of $\mathbb{F}_q$. We fix an algebraic closure K^{alg} of K. Let Γ be a finitely generated $A[F]$-submodule of $\mathbb{G}_a^g(K)$. We denote by $\mathsf{F}(\Gamma)$ and $\mathsf{GF}(\Gamma)$ the F-sets and respectively, the groupless F-sets in Γ based in $\mathbb{G}_a^g(K^{\mathrm{alg}})$. When we do not mention the $A[F]$-submodule containing the base points for the F-sets contained in Γ, we will always understand that the corresponding submodule is $\mathbb{G}_a^g(K^{\mathrm{alg}})$. We will explain in Section 4 that the following Mordell-Lang statement for Drinfeld modules defined over finite fields follows along the same lines as Theorem 7.8 in [3].

Theorem 2.7. *Let $\phi : A \to \mathbb{F}_q[F]$ be a Drinfeld module. Let K be a regular extension of $\mathbb{F}_q$. Let g be a positive integer. Let Γ be a finitely generated $A[F]$-submodule of $\mathbb{G}_a^g(K)$ and let X be an affine subvariety of $\mathbb{G}_a^g$ defined over K. Then $X(K) \cap \Gamma$ is a finite union of F-sets in Γ.*

3. The Mordell-Lang Theorem for semiabelian varieties defined over finite fields

Proof of Theorem 2.5. We first observe that the subgroups Δ_i from the intersection of X with Γ are indeed of the form $G_i(K) \cap \Gamma$ for algebraic groups G_i defined over $\mathbb{F}_q$. Otherwise, we can always replace a subgroup Δ_i appearing in the intersection $X(K) \cap \Gamma$ with its Zariski closure G_i and then intersect with Γ (see also the proof of Lemma 7.4 in [3]). Because G_i is the Zariski closure of a subset of $G(K)$, then G_i is defined over K. Because G_i is an algebraic subgroup of G, then G_i is defined over $\mathbb{F}_q^{\mathrm{alg}}$. Because K is a regular extension of $\mathbb{F}_q$, we conclude that G_i is defined over $\mathbb{F}_q = K \cap \mathbb{F}_q^{\mathrm{alg}}$.

We will prove the main statement of Theorem 2.5 by induction on $\dim(X)$. Clearly, when $\dim(X) = 0$ the statement holds (the intersection is a finite collection of points in that case). Assume the statement holds for $\dim(X) < d$ and we prove that it holds also for $\dim(X) = d$.

We will use in our proof a number of reduction steps.

Step 1. Because $X(K)\cap\Gamma = \overline{X(K)\cap\Gamma}\cap\Gamma$ we may assume that $X(K)\cap\Gamma$ is Zariski dense in X.

Step 2. At the expense of replacing X by one of its irreducible components, we may assume X is irreducible. Each irreducible component of X has Zariski dense intersection with Γ. If our Theorem 2.5 holds for each irreducible component of X, then it also holds for X.

Step 3. We may assume the stabilizer $\mathrm{Stab}_G(X)$ of X in G is finite. Indeed, let $H := \mathrm{Stab}_G(X)$. Then H is defined over K (because X is defined over K) and also, H is defined over $\mathbb{F}_q^{\mathrm{alg}}$ (because it is an algebraic subgroup of G). Thus H is defined over $\mathbb{F}_q$. Let $\pi : G \to G/H$ be the natural projection. Let $\hat{G}$, $\hat{X}$ and $\hat{\Gamma}$ be the images of G, X and Γ through π. Clearly $\hat{\Gamma}$ is a finitely generated subgroup of $\hat{G}(K)$ and also, $\hat{X}$ is defined over K.

If $\dim(H) > 0$, then $\dim(\hat{X}) < \dim(X) = d$. Hence, by the inductive hypothesis, $\hat{X}(K)\cap\hat{\Gamma}$ is a finite union of F-sets in $\hat{\Gamma}$. Using the fact that the kernel of $\pi|_\Gamma$ stabilizes $X(K)\cap\Gamma$, we conclude

$$X(K)\cap\Gamma = \pi|_\Gamma^{-1}\left(\hat{X}(K)\cap\hat{\Gamma}\right),$$

which shows that $X(K)\cap\Gamma$ is also a finite union of F-sets, because $\ker(\pi|_\Gamma)$ is a subgroup of Γ invariant under F (we recall that $\ker(\pi) = H$ is invariant under F).

Therefore, we work from now on under the assumptions that

(i) $\overline{X(K)\cap\Gamma} = X$;

(ii) X is irreducible;

(iii) $\mathrm{Stab}_G(X)$ is finite.

Let $\tilde{\Gamma}$ be the $\mathbb{Z}[F]$-module generated by Γ. Because Γ is finitely generated and F is integral over $\mathbb{Z}$, then also $\tilde{\Gamma}$ is finitely generated. By Theorem 7.8 of [3], $X(K)\cap\tilde{\Gamma}$ is a finite union of F-sets in $\tilde{\Gamma}$. So, there are finitely many groupless F-sets C_i and $\mathbb{Z}[F]$-submodules $H_i \subset \tilde{\Gamma}$ such that

$$X(K)\cap\tilde{\Gamma} = \cup_i\,(C_i + H_i)\,.$$

We want to show $\bigcup_i (C_i + H_i)\cap\Gamma$ is a finite union of F-sets in Γ. It suffices to show that for each i, there exists a finite union B_i of F-sets in Γ such that $(C_i + H_i)\cap\Gamma \subset B_i \subset X(K)$. Indeed, the existence of such B_i yields

$$X(K)\cap\Gamma = \cup_i B_i,$$

as desired.

Case 1. $\dim\overline{C_i + H_i} < d$.

Let $X_i := \overline{C_i + H_i}$. Then X_i is defined over K (because $(C_i + H_i) \subset G(K)$) and $\dim(X_i) < d$. So, by the induction hypothesis, $B_i := X_i(K)\cap\Gamma$ is a finite union of F-sets in Γ. Clearly, $(C_i + H_i)\cap\Gamma \subset B_i \subset X(K)$ (because $X_i \subset X$).

Case 2. $\dim\overline{C_i + H_i} = d$.

Because $X = \overline{X(K)\cap\Gamma}$, then $X = \overline{X(K)\cap\tilde{\Gamma}}$. Moreover, X is irreducible and so, because $\dim\overline{C_i + H_i} = \dim(X)$, then $X = \overline{C_i + H_i}$. Hence $H_i \subset \mathrm{Stab}_G(X)$ because

$$C_i + H_i + H_i = C_i + H_i \text{ and so, } \overline{C_i + H_i} + H_i \subset \overline{C_i + H_i}.$$

Because $\mathrm{Stab}_G(X)$ is finite, we conclude H_i is finite. Thus $(C_i + H_i)$ is a finite union of groupless F-sets because it can be written as a finite union $\cup_{h\in H_i}(h + C_i)$. We let $B_i := (C_i + H_i) \cap \Gamma$. We will show that for each (of the finitely many elements) $h \in H_i$,

$$(h + C_i) \cap \Gamma \text{ is a finite union of groupless } F\text{-sets in } \Gamma. \tag{1}$$

The following lemma will prove (1) and so, it will conclude the proof of Theorem 2.5.

Lemma 3.1. *Let M be a finitely generated $\mathbb{Z}[F]$-submodule of $G(K^{\mathrm{alg}})$ and let $O \in \mathsf{GF}_M$. If Γ is a finitely generated subgroup of $G(K^{\mathrm{alg}})$, then $O \cap \Gamma$ is a finite union of groupless F-sets based in M.*

Proof. If $O \cap \Gamma$ is finite, then we are done. So, from now on, we may assume $O \cap \Gamma$ is infinite. Also, we may and do assume $\Gamma \subset M$ (otherwise we replace Γ with $\Gamma \cap M$).

Let $O := Q + S(P_1, \ldots, P_k; \delta_1, \ldots, \delta_k)$, where $Q, P_1, \ldots, P_k \in M$ and $\delta_i \in \mathbb{N}^*$ for every $i \in \{1, \ldots, k\}$. We may assume that $\delta_1 = \cdots = \delta_k = 1$, in which case $S(P_1, \ldots, P_k; \delta_1, \ldots, \delta_k) := S(P_1, \ldots, P_k; 1)$. Indeed, if we show that

$$(Q + S(P_1, \ldots, P_k; 1)) \cap \Gamma \text{ is a union of groupless } F\text{-sets},$$

then also its subsequent intersection with $(Q + S(P_1, \ldots, P_k; \delta_1, \ldots, \delta_k))$ is a finite union of groupless F-sets, as shown in part (a) of Lemma 3.7 in [3].

Because M is a finitely generated $\mathbb{Z}$-module, M is isomorphic with a direct sum of its finite torsion M_{tor} and a free $\mathbb{Z}$-submodule M_1.

Let

$$f(X) := X^g - \sum_{i=0}^{g-1} \alpha_i X^i \tag{2}$$

be the minimal polynomial for F over $\mathbb{Z}$ (i.e. $f(F) = 0$ in $\mathrm{End}(G)$). Let $r_1, \ldots, r_g$ be all the roots in $\mathbb{C}$ of $f(X)$. Clearly, each $r_i \neq 0$ because F is not a zero-divisor in $\mathrm{End}(G)$. Also, each r_i has absolute value larger than 1 (actually, their absolute values equal q or $q^{\frac{1}{2}}$, according to the Riemann hypothesis for semiabelian varieties defined over $\mathbb{F}_q$). Finally, all r_i are distinct. At most one of the r_i is real and it equals q (and it corresponds to the multiplicative part of G), while all of the other r_i have absolute value equal to $q^{\frac{1}{2}}$ (and they correspond to the abelian part of G). If

$$0 \to T \to G \to A \to 0$$

is a short exact sequence of group varieties, with T being a torus and A an abelian variety, then the roots r_i of absolute value $q^{\frac{1}{2}}$ correspond to roots of the minimal polynomial over $\mathbb{Z}$ for the Frobenius morphism on A. The abelian variety A is isogenuous with a product of simple abelian varieties A_i, all defined over a finite field. If f_i is the minimal polynomial of the corresponding Frobenius on A_i, then the minimal polynomial f_0 of the Frobenius on A is the least common multiple of all f_i. For each i, $\mathrm{End}(A_i)$ is a domain and so, f_i has simple roots. Therefore f_0 (and so, f) has simple roots.

The definition of f shows that for every point $P \in G(K^{\mathrm{alg}})$,

$$F^g P = \sum_{j=0}^{g-1} \alpha_j F^j P. \tag{3}$$

We conclude that for all $n \geq g$,

$$F^n P = \sum_{j=0}^{g-1} \alpha_j F^{n-g+j} P. \tag{4}$$

For each j we define the sequence $\{z_{j,n}\}_{n\geq 0}$ as follows

$$z_{j,n} = 0 \text{ if } 0 \leq n \leq g-1 \text{ and } n \neq j; \tag{5}$$

$$z_{j,j} = 1 \text{ and} \tag{6}$$

$$z_{j,n} = \sum_{l=0}^{g-1} \alpha_l z_{j,n-g+l} \text{ for all } n \geq g. \tag{7}$$

Using (5) and (6) we obtain that

$$F^n P = \sum_{j=0}^{g-1} z_{j,n} F^j P, \text{ for every } 0 \leq n \leq g-1. \tag{8}$$

We prove by induction on n that

$$F^n P = \sum_{j=0}^{g-1} z_{j,n} F^j P, \text{ for every } n \geq 0. \tag{9}$$

We already know (9) is valid for all $n \leq g-1$ due to (8). Thus we assume (9) holds for all $n < N$, where $N \geq g$ and we prove that (9) also holds for $n = N$. Using (4), we get

$$F^N P = \sum_{j=0}^{g-1} \alpha_j F^{N-g+j}. \tag{10}$$

We apply the induction hypothesis to all F^{N-g+j} for $0 \leq j \leq g-1$ and conclude

$$\sum_{j=0}^{g-1} \alpha_j F^{N-g+j} = \sum_{j=0}^{g-1} \alpha_j \sum_{i=0}^{g-1} z_{i,N-g+j} F^i P = \sum_{i=0}^{g-1} \left(\sum_{j=0}^{g-1} \alpha_j z_{i,N-g+j} \right) F^i P. \tag{11}$$

We use (7) in (11) and conclude

$$\sum_{j=0}^{g-1} \alpha_j F^{N-g+j} = \sum_{i=0}^{g-1} z_{i,N} F^i P. \tag{12}$$

Combining (10) and (12) we obtain the statement of (9) for $n = N$. This concludes the inductive proof of (9).

Because $\{z_{j,n}\}_n$ is a recursive defined sequence, then for each $j \in \{0, \ldots, g-1\}$ there exist $\{\gamma_{j,l}\}_{1\leq l\leq g} \subset \mathbb{Q}^{\text{alg}}$ such that for every $n \in \mathbb{N}$,

$$z_{j,n} = \sum_{1\leq l\leq g} \gamma_{j,l} r_l^n. \tag{13}$$

To derive (13) we also use the fact that all r_i are distinct, nonzero numbers.

Equations (9) and (13) show that for every n and for every $P \in G(K^{\text{alg}})$,

$$F^n P = \sum_{0\le j\le g-1} \left(\sum_{1\le l\le g} \gamma_{j,l} r_l^n \right) F^j P. \tag{14}$$

For each $i \in \{1,\dots,k\}$ and for each $j \in \{0,\dots,g-1\}$, let $F^j P_i := T_i^{(j)} + Q_i^{(j)}$, with $T_i^{(j)} \in M_{\text{tor}}$ and $Q_i^{(j)} \in M_1$. Also, let $Q := T_0 + Q_0$, where $T_0 \in M_{\text{tor}}$ and $Q_0 \in M_1$.

Let $R_1,\dots,R_m$ be a basis for the $\mathbb{Z}$-module M_1. For each $j \in \{0,\dots,g-1\}$ and for each $i \in \{1,\dots,k\}$, let

$$Q_i^{(j)} := \sum_{l=1}^{m} a_{i,j}^{(l)} R_l, \tag{15}$$

where $a_{i,j}^{(l)} \in \mathbb{Z}$. Finally, let $a_0^{(1)},\dots,a_0^{(m)} \in \mathbb{Z}$ such that $Q_0 = \sum_{j=1}^{m} a_0^{(j)} R_j$.

For every $n \in \mathbb{N}$ and for every $i \in \{1,\dots,k\}$, (9) and the definitions of $Q_i^{(j)}$ and $T_i^{(j)}$ yield

$$F^n P_i = \sum_{0\le j\le g-1} z_{j,n} \left(T_i^{(j)} + Q_i^{(j)} \right) = \sum_{0\le j\le g-1} z_{j,n} T_i^{(j)} + \sum_{0\le j\le g-1} z_{j,n} Q_i^{(j)}. \tag{16}$$

Because $T_i^{(j)} \in M_{\text{tor}}$, then for each $(n_1,\dots,n_k) \in \mathbb{N}^k$,

$$\sum_{i=1}^{k} \sum_{j=0}^{g-1} z_{j,n_i} T_i^{(j)} \in M_{\text{tor}}.$$

Also, because Q_0 and all $Q_i^{(j)}$ are in M_1 and because $z_{j,n} \in \mathbb{Z}$, then for each $(n_1,\dots,n_k) \in \mathbb{N}^k$,

$$Q_0 + \sum_{i=1}^{k} \sum_{j=0}^{g-1} z_{j,n_i} Q_i^{(j)} \in M_1.$$

Moreover,

$$Q + \sum_{i=1}^{k} F^{n_i} P_i = \left(T_0 + \sum_{\substack{1\le i\le k \\ 0\le j\le g-1}} z_{j,n_i} T_i^{(j)} \right) + \left(Q_0 + \sum_{\substack{1\le i\le k \\ 0\le j\le g-1}} z_{j,n_i} Q_i^{(j)} \right). \tag{17}$$

For each $h \in M_{\text{tor}}$, if $(h + M_1) \cap \Gamma$ is not empty, we fix $(h + U_h) \in \Gamma$ for some $U_h \in M_1$. Let $\Gamma_1 := \Gamma \cap M_1$. Then

$$(h + M_1) \cap \Gamma = h + U_h + \Gamma_1. \tag{18}$$

For each $h \in M_{\text{tor}}$, we let $O_h := \{P \in O \mid P = h + P' \text{ with } P' \in M_1\}$. Then using (18), we get

$$O \cap \Gamma = \bigcup_{h\in M_{\text{tor}}} O_h \cap (h + U_h + \Gamma_1) = \bigcup_{h\in M_{\text{tor}}} \left(h + ((-h + O_h) \cap (U_h + \Gamma_1)) \right). \tag{19}$$

Clearly, $(-h + O_h) \in M_1$. Therefore (19) and (17) yield

$$O \cap \Gamma = \bigcup_{\substack{h\in M_{\text{tor}} \\ T_0 + \sum_{i,j} z_{j,n_i} T_i^{(j)} = h}} \left(h + \left(\left(Q_0 + \sum_{i,j} z_{j,n_i} Q_i^{(j)} \right) \bigcap (U_h + \Gamma_1) \right) \right). \tag{20}$$

In (20), the union is over the finitely many torsion points of M_{tor} (M is finitely generated) and it might be that not for each $h \in M_{\text{tor}}$ there is a corresponding nonempty intersection in (20).

Fix $h \in M_{\text{tor}}$. We show that the set of tuples $(n_1, \ldots, n_k) \in \mathbb{N}^k$ for which

$$h = T_0 + \sum_{i,j} z_{j,n_i} T_i^{(j)} \tag{21}$$

is a finite union of cosets of *semigroups* of $\mathbb{N}^k$ (a semigroup of $\mathbb{N}^k$ is the intersection of a subgroup of $\mathbb{Z}^k$ with $\mathbb{N}^k$). Indeed, let $N \in \mathbb{N}^*$ such that $M_{\text{tor}} \subset G[N]$. Because for each $j \in \{0, \ldots, g-1\}$, $z_{j,n}$ is a recursively defined sequence (as shown by (5), (6) and (7)), then the sequence $\{z_{j,n}\}_n$ is eventually periodic modulo N (a recursively defined sequence is eventually periodic modulo any integral modulus). Thus each value taken by $T_0 + \sum_{i,j} z_{j,n_i} T_i^{(j)}$ is attained for tuples $(n_1, \ldots, n_k)$ which belong to a finite union of cosets of semigroups of $\mathbb{N}^k$.

We will prove next that for each fixed $h \in M_{\text{tor}}$, the tuples $(n_1, \ldots, n_k)$ for which

$$\left(Q_0 + \sum_{i,j} z_{j,n_i} Q_i^{(j)} \right) \in (U_h + \Gamma_1) \tag{22}$$

form a finite union of cosets of semigroups of $\mathbb{N}^k$. This will finish the proof of our theorem because this result, combined with the one from the previous paragraph and combined with (20), will show that the tuples $(n_1, \ldots, n_k)$ for which

$$Q + \sum_{i=1}^{k} F^{n_i} P_i \in \Gamma$$

form a finite union of cosets of semigroups of $\mathbb{N}^k$ (we are also using the fact that the intersection of two finite unions of cosets of semigroups is also a finite union of cosets of semigroups). Lemma 3.4 of [3] shows that the set of points in O corresponding to a finite union of cosets of semigroups containing the tuples of exponents $(n_1, \ldots, n_k)$ is a finite union of groupless F-sets.

Because $\Gamma_1 \subset M_1$ and M_1 is a free $\mathbb{Z}$-module with basis $\{R_1, \ldots, R_m\}$, we can find (after a possible relabelling of $R_1, \ldots, R_m$) a $\mathbb{Z}$-basis $V_1, \ldots, V_n$ ($n \leq m$) of Γ_1 of the following form:

$$V_1 = \beta_1^{(i_1)} R_{i_1} + \cdots + \beta_1^{(m)} R_m;$$

$$V_2 = \beta_2^{(i_2)} R_{i_2} + \cdots + \beta_2^{(m)} R_m;$$

and in general, $V_j = \beta_j^{(i_j)} R_{i_j} + \cdots + \beta_j^{(m)} R_m$, where

$$1 \leq i_1 < i_2 < \cdots < i_n \leq m$$

and all $\beta_j^{(i)} \in \mathbb{Z}$. We also assume $\beta_j^{(i_j)} \neq 0$ for every $j \in \{1, \ldots, n\}$ ($n \geq 1$ because we assumed the intersection $O \cap \Gamma$ is infinite, which means Γ_1 is infinite, because otherwise $|O \cap \Gamma| \leq |M_{\text{tor}}|$).

Let $b_0^{(1)}, \ldots, b_0^{(m)} \in \mathbb{Z}$ such that $U_h = \sum_{j=1}^{m} b_0^{(j)} R_j$. Then a point

$$P := \sum_{j=1}^{m} c^{(j)} R_j \in (U_h + \Gamma_1)$$

if and only if there exist integers $k_1, \ldots, k_n$ such that

$$P = U_h + \sum_{i=1}^{n} k_i V_i. \tag{23}$$

Using the expressions of the V_i, U_h and P in terms of the $\mathbb{Z}$-basis $\{R_1, \ldots, R_m\}$ of M_1, we obtain the following relations:

$$c^{(j)} = b_0^{(j)} \text{ for every } 1 \leq j < i_1; \tag{24}$$

$$c^{(j)} = b_0^{(j)} + k_1\beta_1^{(j)} \text{ for every } i_1 \leq j < i_2; \tag{25}$$

$$c^{(j)} = b_0^{(j)} + k_1\beta_1^{(j)} + k_2\beta_2^{(j)} \text{ for every } i_2 \leq j < i_3 \tag{26}$$

and so on, until

$$c^{(m)} = b_0^{(m)} + \sum_{i=1}^{n} k_i\beta_i^{(m)}. \tag{27}$$

We express equation (25) for $j = i_1$ as a linear congruence modulo $\beta_1^{(i_1)}$ and obtain

$$c^{(i_1)} \equiv b_0^{(i_1)} \left(\text{ mod } \beta_1^{(i_1)} \right). \tag{28}$$

Also from (25) for $j = i_1$, we get $k_1 = \frac{c^{(i_1)} - b_0^{(i_1)}}{\beta_1^{(i_1)}}$. Then we substitute this formula for k_1 in (25) for all $i_1 < j < i_2$ and obtain

$$c^{(j)} = b_0^{(j)} + \frac{c^{(i_1)} - b_0^{(i_1)}}{\beta_1^{(i_1)}}\beta_1^{(j)} \text{ for every } i_1 < j < i_2. \tag{29}$$

Then we express (26) for $j = i_2$ as a linear congruence modulo $\beta_2^{(i_2)}$ (also using the expression for k_1 computed above). We obtain

$$c^{(i_2)} \equiv b_0^{(i_2)} + \frac{c^{(i_1)} - b_0^{(i_1)}}{\beta_1^{(i_1)}}\beta_1^{(i_2)} \left(\text{ mod } \beta_2^{(i_2)} \right). \tag{30}$$

Next we equate k_2 from (26) for $j = i_2$ (also using the formula for k_1) and obtain

$$k_2 = \frac{c^{(i_2)} - b_0^{(i_2)} - \frac{c^{(i_1)} - b_0^{(i_1)}}{\beta_1^{(i_1)}}\beta_1^{(i_2)}}{\beta_2^{(i_2)}}$$

Then we substitute this formula for k_2 in (26) for $i_2 < j < i_3$ and obtain

$$c^{(j)} = b_0^{(j)} + \frac{c^{(i_1)} - b_0^{(i_1)}}{\beta_1^{(i_1)}} \cdot \beta_1^{(j)} + \frac{c^{(i_2)} - b_0^{(i_2)} - \frac{c^{(i_1)} - b_0^{(i_1)}}{\beta_1^{(i_1)}}\beta_1^{(i_2)}}{\beta_2^{(i_2)}} \cdot \beta_2^{(j)}. \tag{31}$$

We go on as above until we express $c^{(m)}$ in terms of

$$c^{(i_1)}, \ldots, c^{(i_n)}$$

and $b_0^{(m)}$ and the $\beta_j^{(l)}$. We observe that all congruences can be written as linear congruences over $\mathbb{Z}$. For example, the above congruence equation (30) modulo $\beta_2^{(i_2)}$ can be written as the following linear congruence over $\mathbb{Z}$:

$$\beta_1^{(i_1)} \cdot c^{(i_2)} \equiv \left(c^{(i_1)} - b_0^{(i_1)}\right) \beta_1^{(i_2)} + \beta_1^{(i_1)} b_0^{(i_2)} \left(\bmod \beta_1^{(i_1)} \cdot \beta_2^{(i_2)}\right).$$

Hence all the above conditions are either linear congruences or linear equations for the $c^{(j)}$.

A typical intersection point from the inner intersection in (20) corresponding to a tuple $(n_1, \ldots, n_k) \in \mathbb{N}^k$ is

$$\left(Q_0 + \sum_{i,j} z_{j,n_i} Q_i^{(j)}\right) \cap (U_h + \Gamma_1)$$

and it can be written in the following form (see also (13)):

$$\sum_{l=1}^{g} \left(a_0^{(l)} + \sum_{\substack{1 \le i \le k \\ 0 \le j \le g-1}} a_{i,j}^{(l)} \sum_{e=1}^{g} \gamma_{j,e} r_e^{n_i} \right) R_l.$$

Such a point lies in $(U_h + \Gamma_1)$ if and only if its coefficients

$$a_0^{(l)} + \sum_{\substack{1 \le i \le k \\ 0 \le j \le g-1}} a_{i,j}^{(l)} \sum_{e=1}^{g} \gamma_{j,e} r_e^{n_i}$$

with respect to the $\mathbb{Z}$-basis $\{R_1, \ldots, R_m\}$ of M_1 satisfy the linear congruences and linear equations such as (24), (28), (29), (30) and (31), associated to $(U_h + \Gamma_1)$. A linear equation as above yields an equation of the following form (after collecting the coefficients of $r_e^{n_i}$ for each $1 \le e \le g$ and each $1 \le i \le k$):

$$\sum_{e=1}^{g} \sum_{i=1}^{k} d_{e,i} r_e^{n_i} = D. \tag{32}$$

All $d_{e,i}$ and D are algebraic numbers. A tuple $(n_1, \ldots, n_k) \in \mathbb{N}^k$ satisfying (32) corresponds to an intersection point of the linear variety L in $(\mathbb{G}_m^g)^k (\mathbb{Q}^{\mathrm{alg}})$ given by the equation

$$\sum_{e=1}^{g} \sum_{i=1}^{k} d_{e,i} X_{e,i} = D \tag{33}$$

and the finitely generated subgroup G_0 of $(\mathbb{G}_m^g)^k (\mathbb{Q}^{\mathrm{alg}})$ spanned by

$$(r_1, \ldots, r_g, 1, \ldots, 1);\ (1, \ldots, 1, r_1, \ldots, r_g, 1, \ldots, 1);\ \ldots, (1, \ldots, 1, r_1, \ldots, r_g). \tag{34}$$

Each vector in (34) has gk components. There are k multiplicatively independent generators above for G_0 (we are using the fact that $|r_i| > 1$, for each i). Hence $G_0 \simeq \mathbb{Z}^k$. By Lang Theorem for $\mathbb{G}_m^{gk}$, we conclude the intersection of $L(\mathbb{Q}^{\mathrm{alg}})$ and G_0 is a finite union of cosets of subgroups of G_0. The subgroups of G_0 correspond to subgroups of $\mathbb{Z}^k$. Hence the tuples $(n_1, \ldots, n_k) \in \mathbb{N}^k$ which satisfy (32) belong to a finite union of cosets of semigroups of $\mathbb{N}^k$.

A congruence equation as (28) or (30), corresponding to conditions for a point to lie in $(U_h + \Gamma_1)$ yields a congruence relation between the coefficients (with respect to the $\mathbb{Z}$-basis

$\{R_1, \ldots, R_m\}$ of M_1) of a typical point of the form $Q_0 + \sum_{j,i} z_{j,n_i} Q_i^{(j)}$. We will show that such tuples $(n_1, \ldots, n_k)$ belong to a finite union of cosets of semigroups of $\mathbb{N}^k$.

The coefficient of R_l in $\left(Q_0 + \sum_{j,i} z_{j,n_i} Q_i^{(j)}\right)$ can be written as (see also (15))

$$a_0^{(l)} + \sum_{\substack{1 \le i \le k \\ 0 \le j \le g-1}} a_{i,j}^{(l)} z_{j,n_i}. \tag{35}$$

Hence a congruence equation corresponding to a point of the form $\left(Q_0 + \sum_{j,i} z_{j,n} Q_i^{(j)}\right)$ which also lies in $(U_h + \Gamma_1)$ has the form

$$\sum_{j=0}^{g-1} \sum_{i=1}^{k} d_{j,i} z_{j,n_i} \equiv D_1 (\bmod\ D_2) \tag{36}$$

for some integers $d_{j,i}$ (we recall that $a_{i,j}^{(l)} \in \mathbb{Z}$), D_1 and $D_2 \neq 0$. Recursively defined sequences as $\{z_{j,n}\}_n$ are eventually periodic modulo any nonzero integer (hence, they are eventually periodic modulo D_2). Therefore all the solutions $(n_1, \ldots, n_k)$ to (36) belong to a finite union of cosets of semigroups of $\mathbb{N}^k$.

Hence for each $h \in M_{\text{tor}}$ the tuples $(n_1, \ldots, n_k) \in \mathbb{N}^k$ for which

$$\left(Q_0 + \sum_{i,j} z_{j,n_i} Q_i^{(j)}\right) \in (U_h + \Gamma_1),$$

form a finite union of cosets of semigroups of $\mathbb{N}^k$. We also proved that for each $h \in M_{\text{tor}}$ the tuples $(n_1, \ldots, n_k) \in \mathbb{N}^k$ for which

$$h = T_0 + \sum_{i,j} z_{j,n_i} T_i^{(j)},$$

form a finite union of cosets of semigroups of $\mathbb{N}^k$. In conclusion, we get that

$$\left(Q + \sum_{i=1}^{k} F^{n_i} P_i\right) \in \Gamma$$

if and only if $(n_1, \ldots, n_k)$ belongs to a finite union of cosets of semigroups of $\mathbb{N}^k$. The corresponding subset of $(Q + S(P_1, \ldots, P_k; 1))$ for a finite union of cosets of semigroups of $\mathbb{N}^k$ is precisely a finite union of groupless F-sets based in M (as shown by Lemma 3.4 of [3]).

This concludes the proof of Lemma 3.1 □

As remarked before the statement of Lemma 3.1, this lemma concludes the proof of our Theorem 2.5. □

4. The Mordell-Lang Theorem for Drinfeld modules defined over finite fields

The setting for this section is that $\phi : A \to \mathbb{F}_q[F]$ is a Drinfeld module.

The following result (which is the equivalent for Drinfeld modules of Lemma 7.5 in [3]) will be used in the proof of our Theorem 2.7.

Lemma 4.1. *Let K be a finitely generated field extension of $\mathbb{F}_q$ and let $\Gamma \subset \mathbb{G}_a^g(K)$ be a finitely generated $A[F]$-submodule.*

(a) The F-pure hull of Γ in $\mathbb{G}_a^g(K)$, i.e. the set of all $x \in \mathbb{G}_a^g(K)$ such that $F^m x \in \Gamma$ for some $m \geq 0$, is a finitely generated A-module. In particular, Γ is a finitely generated A-module.

(b) For each $m > 0$, $\Gamma / F^m\Gamma$ is finite.

(c) There exists $m \geq 0$ such that $\Gamma \setminus F\Gamma \subset \mathbb{G}_a^g(K) \setminus \mathbb{G}_a^g\left(K^{q^m}\right)$.

Proof. (a) First we observe that the F-pure hull $\tilde{\Gamma}$ of Γ is an $A[F]$-module, and so, implicitly an A-module. Indeed, if $x \in \tilde{\Gamma}$ and $m \in \mathbb{N}$ such that $F^m x \in \Gamma$, then for every $f \in A[F]$,

$$F^m(f(x)) = f(F^m x) \in f(\Gamma) \subset \Gamma.$$

Therefore $f(x) \in \tilde{\Gamma}$, showing that $\tilde{\Gamma}$ is an $A[F]$-module.

It suffices to prove (a) under the extra assumption that $\Gamma = \Gamma_0^g$ (the cartesian product of Γ_0 with itself g times), where $\Gamma_0 \subset K$ is a finitely generated $A[F]$-module. Indeed, let Γ_0 be the finitely generated $A[F]$-submodule of K spanned by all the generators (over $A[F]$) of the projections of Γ on the g coordinates of $\mathbb{G}_a^g(K)$. Clearly $\Gamma \subset \Gamma_0^g$ and if we prove (a) for Γ_0, then the result of (a) holds also for Γ_0^g and implicitly for its submodule Γ (the F-pure hull of Γ is an A-submodule of the F-pure hull of Γ_0^g and a submodule of a finitely generated module over a Dedekind domain is also finitely generated). So, we are left to show that the F-pure hull $\tilde{\Gamma}_0$ of Γ_0 in K is a finitely generated A-module.

By its construction, Γ_0 is a finitely generated $A[F]$-submodule of K. Because F is integral over A, we conclude Γ_0 is also finitely generated as an A-module. As explained in the beginning of our proof, $\tilde{\Gamma}_0$ is also an A-module. We first prove $\tilde{\Gamma}_0$ lies inside the A-division hull Γ_0' of Γ_0 in K. Indeed, let $x \in \tilde{\Gamma}_0$ and let $m \in \mathbb{N}$ such that $F^m x \in \Gamma_0$. We will prove next that $x \in \Gamma_0'$.

Because F is integral over A, then also F^m is integral over A. Let $s \in \mathbb{N}^*$ and let $\alpha_0, \ldots, \alpha_{s-1} \in A$ such that

$$F^{sm} = \sum_{i=0}^{s-1} \alpha_i F^{i \cdot m} \text{ in } \mathrm{End}(\phi). \tag{37}$$

Because $A[F]$ is a domain, we may assume $\alpha_0 \neq 0$ (otherwise we would divide (37) by powers of F^m until the coefficient of F^0 would be nonzero). Equality (37) shows that

$$\phi_{\alpha_0}(x) = F^{sm}x - \sum_{i=1}^{s-1} \phi_{\alpha_i}\left(F^{i\cdot m}x\right) \in \Gamma_0, \tag{38}$$

because $F^m x \in \Gamma_0$ and Γ_0 is an $A[F]$-module. Thus (38) shows x belongs to the A-division hull Γ_0'. Let $F_0 := \mathrm{Frac}(A)$. Because $\tilde{\Gamma}_0 \subset \Gamma_0'$ and because Γ_0 is a finitely generated A-module, we conclude

$$\dim_{F_0}\left(\tilde{\Gamma}_0 \otimes_A F_0\right) \leq \dim_{F_0}\left(\Gamma_0' \otimes_A F_0\right) < \aleph_0. \tag{39}$$

Hence (39) shows $\tilde{\Gamma}_0$ has *finite rank* as an A-module. Lemma 4 of [5] shows that every finite rank A-module is finitely generated. This concludes the proof of (a).

(b) Because Γ is a finitely generated $A[F]$-module, then $\Gamma / F^m\Gamma$ is a finitely generated $A[F]/(F^m)$-module. Hence, it suffices to show $A[F]/(F^m)$ is a finite ring. Let, as before,

(37) be the minimal equation of F^m over A. Then $\alpha_0 \in F^m \cdot A[F]$. So, $A[F]/(F^m)$ is a quotient of $A[F]/(\alpha_0)$. Clearly, $A[F]/(\alpha_0) \simeq (A/(\alpha_0))[F]$. Because $\alpha_0 \neq 0$ and A is a Dedekind domain for which the residue field for each nonzero ideal is finite, we conclude $A/(\alpha_0)$ is finite (we know that $A/\mathfrak{p}$ is finite for every nonzero prime ideal $\mathfrak{p}$, but every nonzero ideal in A is a product of nonzero prime ideals). Because F is integral over A we conclude $(A/(\alpha_0))[F]$ is finite. Hence $A[F]/(F^m)$ is finite and so, $\Gamma/F^m\Gamma$ is finite, as desired.

(c) Because the F-pure hull $\tilde{\Gamma}$ of Γ in $\mathbb{G}_a^g(K)$ is finitely generated as an $A[F]$-module, then there exists $m_0 > 0$ such that $F^{m_0}\tilde{\Gamma} \subset \Gamma$. Let $m := m_0 + 1$. Then

$$\Gamma \cap \mathbb{G}_a^g\left(K^{q^m}\right) \subset F^m\tilde{\Gamma} \subset F\Gamma.$$

Hence $\Gamma \setminus F\Gamma \subset \mathbb{G}_a^g(K) \setminus \mathbb{G}_a^g\left(K^{q^m}\right)$. □

We will also use in our proof of Theorem 2.7 the following result on the combinatorics of the F-sets.

Lemma 4.2. *Suppose K is a regular field extension of $\mathbb{F}_q$, $\Gamma \subset \mathbb{G}_a^g(K)$ is a finitely generated $A[F]$-module, $X \subset \mathbb{G}_a^g$ is an affine variety defined over K and $b \in \mathbb{N}^*$. Clearly Γ is an $A[F^b]$-module as well. If $U \subset \Gamma$ is an F^b-set with $U \subset X(K)$, then there exists $V \in \mathsf{F}(\Gamma)$ such that $U \subset V \subset X(K)$. In particular, if $X(K) \cap \Gamma$ is a finite union of F^b-sets, then it is also a finite union of F-sets.*

Proof. Our proof follows the proof of its similar statement for semiabelian varieties instead of Drinfeld modules and for $\mathbb{Z}[F]$ instead of $A[F]$ (Lemma 7.4 of [3]).

Let $U = C + \Delta$, where C is a groupless F^b-set and Δ is a subgroup of Γ invariant under F^b. Let H be the Zariski closure of Δ in $\mathbb{G}_a^g$. Then H is invariant under F^b. Hence H is defined over $\mathbb{F}_{q^b}$ (which is the fixed field of F^b). Because H is the Zariski closure of a subset of $\mathbb{G}_a^g(K)$, then H is defined over K. Therefore H is defined over $K \cap \mathbb{F}_{q^b}$. Because K is a regular extension of $\mathbb{F}_q$, then $K \cap \mathbb{F}_{q^b} = \mathbb{F}_q$. Thus H is defined over $\mathbb{F}_q$ and so, $H(K) \cap \Gamma$ is invariant under F.

Clearly every groupless F^b-set is also a groupless F-set and so, C is a groupless F-set. Therefore we conclude that $V := C + H(K) \cap \Gamma$ is an F-set in Γ, which contains U. On the other hand, $H \subset X$ (because $\Delta \subset X(K)$ and $H = \overline{\Delta}$). Moreover, for each $c \in C$,

$$c + H(K) \cap \Gamma \subset \overline{c + \Delta}(K) \subset X(K).$$

Thus $V \subset X(K)$, as desired. □

The proof of the next two lemmas are identical with the proofs of Corollary 7.3 and respectively, Lemma 3.9 in [3].

Lemma 4.3. *Suppose $\Gamma \subset \mathbb{G}_a^g(K)$ is a finitely generated $A[F]$-module, U is a finite union of F-sets in Γ and $X \subset \mathbb{G}_a^g$ is an affine variety defined over K. Let $\Sigma := \bigcup_{n\geq 0} F^n U$ and suppose that $\Sigma \subset X(K)$. Then there exists a finite union B of F-sets in Γ such that $\Sigma \subset B \subset X(K)$.*

Lemma 4.4. *Suppose M is a finitely generated $A[F]$-module.*

(a) The intersection of two finite unions of F-sets in M is also a finite union of F-sets in M.

(b) If X is a finite union of F-sets in M and N is a submodule of M, then $X \cap N$ is a finite union of F-sets in N.

We will deduce Theorem 2.7 from the following slightly more general statement (our Theorem 2.7 is a particular case of Theorem 4.5 for $H = \{0\}$).

Theorem 4.5. *Let K be a regular extension of $\mathbb{F}_q$. Let H be any algebraic subgroup of $\mathbb{G}_a^g$ defined over $\mathbb{F}_q$. Then for every variety $X \subset \mathbb{G}_a^g/H$ defined over K and for every finitely generated $A[F]$-submodule $\Gamma \subset (\mathbb{G}_a^g/H)(K)$, the intersection $X(K) \cap \Gamma$ is a finite union of F-sets in Γ based in $(\mathbb{G}_a^g/H)(K^{\mathrm{alg}})$.*

Proof. We first observe that because H is an algebraic group defined over $\mathbb{F}_q$, then H is invariant under $A[F]$. Hence, the quotient $\mathbb{G}_a^g/H$ is equipped with a natural A-action.

Our proof follows the proof of Theorem 7.8 of [3]. Because ϕ is defined over a finite field and because Γ is a finitely generated A-module (see (a) of Lemma 4.1) and because X is defined over a finitely generated field, then there exists a finitely generated subfield L of K such that X is defined over L and $\Gamma \subset \mathbb{G}_a^g(L)$. Therefore we may and do assume that K is finitely generated.

We will use induction on $\dim(X)$. If $\dim(X) = 0$, then $X(K) \cap \Gamma$ is a finite collection of points. Clearly, each point is an F-set. We assume that Theorem 4.5 holds for $\dim(X) < n$ (for some $n \geq 1$) and we will prove that it also holds for $\dim(X) = n$.

We may assume $\overline{X(K) \cap \Gamma} = X$ (otherwise, we may replace X with $\overline{X(K) \cap \Gamma}$). Also, we may assume X is irreducible because it suffices to prove Theorem 4.5 for each irreducible component of X (we are using the fact that the intersection of X with Γ is Zariski dense if and only if the intersection of each irreducible component of X with Γ is Zariski dense in that component).

The next lemma shows that a translate of X is defined over a finite field. The proof of Lemma 4.6 is almost identical with the proof of Lemma 7.7 in [3]. Lemma 7.7 in [3] holds for any finitely generated subgroup of a semiabelian variety. In particular, it holds for any finitely generated $\mathbb{Z}[F]$-submodule of a semiabelian variety. The only difference between Lemma 7.7 in [3] and our Lemma 4.6 is that in [3], Γ can be taken to be a module over the Frobenius ring $\mathbb{Z}[F]$ (associated to a semiabelian variety defined over a finite field), while in our case, Γ is a module over the Frobenius ring $A[F]$ (associated to a Drinfeld module defined over a finite field). The only property of the Frobenius ring used in the proof of Lemma 7.7 in [3] is property (b) from Lemma 4.1 and the only property of the ambient algebraic group G (a semiabelian variety in [3] and $\mathbb{G}_a^g/H$ for us) used in the proof of Lemma 7.7 in [3] is that $\bigcap_{n\geq 1} F^n G(K^{\mathrm{alg}}) = G(\mathbb{F}_q^{\mathrm{alg}})$.

Lemma 4.6. *Suppose Γ is a finitely generated $A[F]$-submodule of $(\mathbb{G}_a^g/H)(K)$ and $X \subset (\mathbb{G}_a^g/H)$ is a variety defined over K such that $X(K) \cap \Gamma$ is Zariski dense in X. Then for some $\gamma \in K^{\mathrm{alg}}$, $(\gamma + X)$ is defined over $\mathbb{F}_q^{\mathrm{alg}}$.*

Next we show that we may assume X is defined over $\mathbb{F}_q$. Lemma 4.6 shows that there exists $\gamma \in K^{\mathrm{alg}}$ such that $(\gamma + X)$ is defined over $\mathbb{F}_q^{\mathrm{alg}}$. Let Γ' be the finitely generated $A[F]$-module generated by γ and the elements of Γ. Let $K' := K(\gamma)$. Because $X(K) \cap \Gamma$ is Zariski dense in X, then $(\gamma + X) \cap \Gamma'$ is Zariski dense in $(\gamma + X)$. Hence $(\gamma + X)$ is defined over K'. But we already know that $(\gamma + X)$ is defined over $\mathbb{F}_q^{\mathrm{alg}}$. Hence $(\gamma + X)$ is defined over

$$\mathbb{F}_{q^b} := K' \cap \mathbb{F}_q^{\mathrm{alg}}.$$

Assuming the statement of our Theorem 4.5 valid for varieties defined over the finite field fixed by the Frobenius, we obtain that $(\gamma + X) \cap \Gamma'$ is an F^b-set. Because Γ is an $A[F^b]$-submodule of Γ', we conclude

$$X(K) \cap \Gamma = X(K') \cap \Gamma = (X(K') \cap \Gamma') \cap \Gamma.$$

Hence, using part (b) of Lemma 4.4, $X(K) \cap \Gamma$ is an F^b-set in Γ. An application of Lemma 4.2 concludes the proof that $X(K) \cap \Gamma$ is indeed an F-set in Γ. Therefore, from now on, we assume that X is defined over $\mathbb{F}_q$.

We may also assume $\mathrm{Stab}(X) \subset \mathbb{G}_a^g/H$ is trivial. Indeed, let $H_1 = \mathrm{Stab}(X)$. Then H_1 is defined over the same field as X. Hence H_1 is defined over $\mathbb{F}_q$. We consider the canonical quotient map $\pi : (\mathbb{G}_a^g/H) \to \mathbb{G}_a^g/(H + H_1)$. Let $\hat{X}$ and $\hat{\Gamma}$ be the images of X and Γ through π. Clearly $\mathrm{Stab}(\hat{X}) = \{0\}$. Moreover, if Theorem 4.5 holds for $\hat{X}(K) \cap \hat{\Gamma}$, then it also holds for $X(K) \cap \Gamma = \pi|_{\Gamma}^{-1}\left(\hat{X}(K) \cap \hat{\Gamma}\right)$ (we use the fact that $\ker(\pi|_{\Gamma}) = \Gamma \cap H_1(K)$ is a subgroup of Γ invariant under F). Also, it is precisely this part of our proof where we need the hypothesis of Theorem 4.5 be that X is a subvariety of a quotient of $\mathbb{G}_a^g$ through an algebraic subgroup defined over $\mathbb{F}_q$.

From this point on the proof of Theorem 4.5 is identical with the proof of Theorem 7.8 in [3] (we provided in Lemmas 4.1, 4.2 and 4.3 the technical ingredients that are used in the argument from the proof of Theorem 7.8 in [3]). □

The following result follows from Theorem 3.1 in [4] the same way our Theorem 2.7 followed from Theorem 7.8 in [3].

Theorem 4.7. *Let $\phi : A \to \mathbb{F}_q[F]$ be a Drinfeld module. Let F be the Frobenius on $\mathbb{F}_q$. Let K be an algebraically closed field extension of $\mathbb{F}_q$. Let $X \subset \mathbb{G}_a^g$ (for some $g \geq 1$) be an affine variety defined over K. Let $\Gamma \subset \mathbb{G}_a^g(K)$ be a finitely generated $A[F]$-module. Let $\Gamma' := \Gamma + \mathbb{G}_a^g(\mathbb{F}_q^{\mathrm{alg}})$. Then $X(K) \cap \Gamma'$ is a finite union of sets of the form $\left(U + Y(\mathbb{F}_q^{\mathrm{alg}})\right)$, where $U \subset \Gamma'$ is an F^b-set for some $b \in \mathbb{N}^*$ and $Y \subset \mathbb{G}_a^g$ is an affine variety defined over $\mathbb{F}_q^{\mathrm{alg}}$.*

In the following Example 4.8, we extend the notion of Drinfeld modules defined over finite fields and then we show that for our *new* Drinfeld modules, the groups appearing in the intersection from the conclusion of Theorem 2.7 are not necessarily A-modules (and hence, they are not $A[F]$-modules). This is in contrast with the semiabelian case where the groups appearing in the intersection $X(K) \cap \Gamma$ are $\mathbb{Z}[F]$-modules.

Example 4.8. Let $a \in \mathbb{N}^*$. Let K be a regular extension of $\mathbb{F}_{q^a}$. Let $\mathbb{F}_{q^a}\{F\}$ be the ring of twisted polynomials in F with coefficients in $\mathbb{F}_{q^a}$ (the addition is the usual one, while the multiplication is the composition of functions). A Drinfeld module over a finite field is a ring homomorphism $\phi : A \to \mathbb{F}_{q^a}\{F\}$ for which there exists $a \in A$ such that $\phi_a \notin \mathbb{F}_{q^a} \cdot F^0$. Then F is not necessarily an endomorphism for ϕ, but $F^a \in \mathrm{End}(\phi)$. We want to characterize the intersections $X(K) \cap \Gamma$, where $X \subset \mathbb{G}_a^g$ is an affine variety defined over K and $\Gamma \subset \mathbb{G}_a^g(K)$ is a finitely generated $A[F^a]$-submodule.

We cannot always expect that the subgroups of Γ appearing in $X(K) \cap \Gamma$ be actually A-submodules. For example, let $C = \mathbb{P}^1_{\mathbb{F}_q}$ and let $A = \mathbb{F}_q[t]$. Let $a = 2$. Define $\phi : A \to \mathbb{F}_{q^2}\{F\}$ by $\phi_t = F + F^3$. Let $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Consider the curve $X \subset \mathbb{G}_a^2$ defined by $y = \lambda x$. Let $K = \mathbb{F}_{q^2}(t)$ and let $\Gamma \subset \mathbb{G}_a^2(K)$ be the cyclic $A[F^2]$-submodule generated by $(t, \lambda t)$.

Then $X(K) \cap \Gamma$ consists of all points in Γ of the form $(f(t), f(\lambda t))$, where $f \in A[F^2]$ is a polynomial in F^2 with coefficients in $\mathbb{F}_q$. In particular, $X(K) \cap \Gamma$ is invariant under $\phi_{t^2} = F^2 + 2F^4 + F^6$, but it is not invariant under ϕ_t. So, the intersection is an $\mathbb{F}_q[F^2]$-submodule of Γ, but not an $A[F^2]$-submodule.

The following example shows that we cannot obtain a similar statement as our Theorem 2.5 in the context of Drinfeld modules, i.e. we cannot replace the $A[F]$-submodules Γ in Theorem 2.7 with simply A-modules.

Example 4.9. Assume q is odd and let $A = \mathbb{F}_q[t]$. Define $\phi : A \to \mathbb{F}_q[F]$ by $\phi_t = F + F^2$.

Let $Y \subset \mathbb{G}_a^g$ be a smooth curve defined over $\mathbb{F}_q$ and let $K := \mathbb{F}_q(Y)$. Let $P \in Y(K)$ be a generic point for Y. Define $X := \overline{Y + Y}$ and assume X does not contain translates of nontrivial algebraic subgroups of $\mathbb{G}_a^g$ (for *generic* curves Y this is always possible). Let $\tilde{\Gamma}$ be the $A[F]$-submodule of $\mathbb{G}_a^g(K)$ generated by P. Then, using that X does not contain a translate of a nontrivial algebraic subgroup of $\mathbb{G}_a^g$, we conclude

$$X(K) \cap \tilde{\Gamma} = S(P, P; 1). \tag{40}$$

Let Γ be the cyclic A-module generated by P. Clearly, $\Gamma \subset \tilde{\Gamma}$. Hence, using (40), we obtain

$$X(K) \cap \Gamma = \bigcup_{n \geq 0} \phi_{t^{p^n}}(P) = \bigcup_{n \geq 0} \left(F^{p^n} P + F^{2p^n} P \right).$$

This is the case because the only elements $a \in A$ such that $\phi_a = F^n + F^m$ are of the form $a = t^{p^n}$ (this is an easy exercise in combinatorics, whose proof we provide below for completeness).

Lemma 4.10. *Assume p is an odd prime and let q be a power of p. Let $A := \mathbb{F}_q[t]$ and define the Drinfeld module $\phi : A \to \mathbb{F}_q[F]$ by $\phi_t = F + F^2$. Then the only elements $a \in A$ such that ϕ_a equals $F^n + F^m$ for some $n, m \in \mathbb{N}$ are of the form $a = t^{p^n}$ (in which case $\phi_{t^{p^n}} = F^{p^n} + F^{2p^n}$.*

Proof. Let $a = \sum_{i=0}^{n} a_i t^i \in A$ (hence $a_i \in \mathbb{F}_q$). Assume ϕ_a is the sum of two powers of F. We will prove that all $a_i = 0$ for $i < n$ and also that n is a power of p.

First we observe that if $a_i = 0$ for all $i < n$, then $a = a_n t^n$ and so, the expansion of $(F + F^2)^n$ contains *only* two powers of F if and only if n is a power of p (Lucas Theorem for Binomial Congruences). Moreover, $a_n = 1$ in order for ϕ_a to be a sum of two powers of F.

Assume there is $k < n$ such that $a_k \neq 0$. Let m be the least such k. Then the term $a_m F^m$ has the smallest power of F which appears in ϕ_a (and it is not cancelled by any other term in ϕ_a). On the other hand, $a_n F^{2n}$ is the term in ϕ_a with the largest power of F (and also it is not cancelled by any other term in ϕ_a). Therefore the only two powers of F in ϕ_a are F^m and F^{2n}.

Let l be the index of the first nonzero digit in the expansion of n in base p, i.e.

$$n = \sum_{j \geq l} \alpha_j p^j$$

and $\alpha_l \neq 0$. Then the coefficient of F^{2n-p^l} in the expansion $\phi_{a_n t^n}$ equals $a_n \binom{n}{p^l} \neq 0$ in $\mathbb{F}_q$ (by Lucas Theorem for Binomial Congruences). Moreover, also by Lucas Theorem, we get that

F^{2n-p^l} is the largest power of F, not equal to F^{2n}, which appears with nonzero coefficient in the expansion of $\phi_{a_n t^n}$. Also,

$$2n - p^l \geq n > m.$$

Thus the power F^{2n-p^l} has to be cancelled by another term in ϕ_a. Let $n_1 < n$ be the largest index i such that $a_i \neq 0$. Then the largest power of F in $\phi_{a-a_n t^n}$ is F^{2n_1} which does not cancel F^{2n-p^l}, because p^l is odd. Hence, either the power F^{2n-p^l} or the power F^{2n_1} appear with nonzero coefficients in ϕ_a, contradicting thus the fact that the only powers of F in ϕ_a are F^m and F^{2n}. □

Remark 4.11. The above proof works applied to the Drinfeld module $\phi : \mathbb{F}_q[t] \to \mathbb{F}_q[F]$ defined by $\phi_t = F + F^3$, in case $p = 2$, and shows that the only elements $a \in A$ such that ϕ_a equals $F^n + F^m$ for some $n, m \in \mathbb{N}$ are of the form $a = t^{2^n}$ (in which case $\phi_{t^{2^n}} = F^{2^n} + F^{3 \cdot 2^n}$). This allows us to construct a similar example in characteristic 2 as Example 4.9 for the failure of a Mordell-Lang statement such as Theorem 2.7 for finitely generated A-modules Γ.

References

[1] D. Ghioca, *The Mordell-Lang Theorem for Drinfeld modules*. Internat. Math. Res. Notices, **53**, (2005), 3273-3307.

[2] D. Goss, *Basic structures of function field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 35. Springer-Verlag, Berlin, 1996.

[3] R. Moosa, T. Scanlon, *F-structures and integral points on semiabelian varieties over finite fields*. Amer. Journal of Math., **126** (2004), 473-522.

[4] R. Moosa, T. Scanlon, *The Mordell-Lang Conjecture in positive characteristic revisited*. Model Theory and Applications (eds. L. Bélair, P. D'Aquino, D. Marker, M. Otero, F. Point, & A. Wilkie), 2003, 273-296.

[5] B. Poonen, *Local height functions and the Mordell-Weil theorem for Drinfeld modules*. Compositio Mathematica **97** (1995), 349-368.

Dragos Ghioca, Department of Mathematics & Statistics, Hamilton Hall, Room 218, McMaster University, 1280 Main Street West, Hamilton, Ontario L8S 4K1, Canada

E-mail address: dghioca@math.mcmaster.ca